UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IKASYSTEMS CORPORATION, a Delaware corporation Plaintiff, vs. **BRIJESH KALIDINDI, an individual** Defendant.	Case No. Hon. Preliminary Injunction Requested

COMPLAINT

Plaintiff ikaSystems Corporation ("ikaSystems"), by its undersigned counsel, alleges the following as and for its complaint against Defendant Brijesh Kalidindi ("Kalidindi"):

NATURE OF THE ACTION

This is an action for trade secret misappropriation brought by ikaSystems against its former IT Architect Principal. Brijesh Kalidindi ("Kalidindi") was responsible for developing and implementing a valuable proprietary software service that ikaSystems offers to healthcare insurance companies. During the final ten days of his employment, Kalidindi surreptitiously downloaded and transferred thousands of documents containing ikaSystems' confidential trade secret information, including proprietary source code and software architecture information. Kalidindi transferred these files to at least one personal account on a file-sharing website, in violation of his confidentiality agreement with ikaSystems and ikaSystems' data protection policies. Kalidindi attempted to avoid detection by initiating the file transfers at night while disconnected from ikaSystems' corporate network and erasing the history on his personal drive. Kalidindi may be using ikaSystems' trade secret information in his new employment or for personal gain. Accordingly, Kalidindi's wrongful conduct has caused significant harm to ikaSystems.

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff ikaSystems is a Delaware corporation with a principal place of business in Southborough, Massachusetts.

2. Upon information and belief, Kalidindi is a Michigan citizen who resides in West Bloomfield, Michigan.

3. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1332, as the amount in controversy exceeds $75,000 exclusive of interest and costs, and the adverse parties are citizens of different states. The Court has further subject matter jurisdiction pursuant to 28 U.S.C. §1331 because Plaintiff is asserting claims under the Defend Trade Secrets Act of 2016, 18 U.S.C. §1836, and the Computer Fraud and Abuse Act, 18 U.S.C. §1030, *et seq*.

4. The Court has personal jurisdiction over Defendant because he contracted for employment and worked for ikaSystems, a Massachusetts-based company. In the course of his employment at ikaSystems, Defendant traveled to ikaSystems' Massachusetts office on a near weekly basis. The Court also has personal jurisdiction over Defendant because he expressly consented to personal jurisdiction in this Court in the Non-Competition, Non-Solicitation, and Confidentiality Agreement (the "Agreement") from which this action arises. (See executed Agreement, a true and correct copy of which is attached hereto as **Exhibit 1**, § 15). In pertinent part, the Agreement states:

> Employee agrees that any action or proceeding relating to this Agreement or Employee's employment with ikaSystems must be initiated in a state or federal court located in the Commonwealth of Massachusetts, and that Employee shall submit without objection to the jurisdiction of the Commonwealth of Massachusetts with respect to such action or proceeding. (Ex. 1, § 15.)

5. Venue in this District is proper because Defendant transacts business within the District and Defendant has consented to venue in this District under the Agreement.

STATEMENT OF FACTS

Overview of ikaSystems' Business

6. ikaSystems, formed in 1999, provides software and data solutions for healthcare insurance companies through a proprietary technology platform. The software is utilized by individual clients on a software as a service ("SaaS") basis to deliver cost containment or cost reductions in core business functionalities such as enrollment, billing, and claims processing.

7. ikaSystems is based in Southborough, Massachusetts with employees in Massachusetts, Michigan, and Virginia.

8. ikaSystems developed an Enterprise Payer Platform ("Platform"), a software service that reduces administrative and avoidable medical costs for Medicare and other Federal and State sponsored health care plans.

9. The Platform provides its clients efficiencies in the administrative operation of health insurance plans by offering a platform for enrollment, claims, and billing.

10. In November 2015, Blue Cross Blue Shield of Michigan ("BCBSM"), through a wholly-owned subsidiary acquired ikaSystems as a wholly-owned subsidiary.

11. BCBSM has utilized ikaSystems' Platform to offer business solutions under the brand "Visiant".

ikaSystems Hires Kalidindi as an IT Architect Principal in 2017 to Lead the Development of an Enhanced Platform

12. Kalidindi joined BCBSM in August 2005 as a technology specialist.

13. In February 2017, Kalidindi transferred his employment from BCBSM where he was hired as ikaSystems' "IT Architect Principal."

14. On February 2, 2017, Kalidindi and ikaSystems executed a Non-Competition, Non-Solicitation, and Confidentiality Agreement (**Exhibit 1**, "Agreement").

15. In Section 1 of the Agreement, Kalidindi acknowledged he owed a duty of loyalty to ikaSystems.

16. In Section 5 of the Agreement, Kalidindi acknowledged he would have access to confidential and proprietary information, including trade secrets, and expressly agreed not to use or disclose any of this information for any purpose other than the performance of his essential job duties at ikaSystems.

17. In Section 6 of the Agreement, Kalidindi agreed that all intellectual property developed in the course of his employment, including software code and similar developments, remained ikaSystems' property.

18. In Section 8 of the Agreement, Kalidindi agreed that upon termination, he would return all confidential information, which would include documents, notes, models, and any other data and records of any kind.

19. The Enhanced Platform improved the existing architectural design of ikaSystems' Platform. Among other things, the Enhanced Platform allows for integration with third-party software and is cloud-based.

20. ikaSystems made a substantial financial investment into the research, design, and implementation of the Enhanced Platform, which ikaSystems recently introduced commercially. ikaSystems has invested tens of millions of dollars in the development of the Enhanced Platform.

21. Kalidindi was the lead IT employee on the Enhanced Platform. He was a member of the team of programmers and software architects that researched, designed, modified, and implemented the Enhanced Platform and corresponding software.

ikaSystems' Information Protection Protocols

22. ikaSystems' proprietary software as a service utilizes and handles a substantial amount of confidential and sensitive data. This data includes information protected by federal and state privacy laws, such as protected health information (medical claims, diagnoses, and procedures) and personally identifiable information (social security numbers and addresses) (collectively "PHI"). The applications themselves are valuable proprietary software code that allows for the handling and protection of this information.

23. In order to protect this confidential and sensitive data, as well as other sensitive information of the company, ikaSystems has implemented a strict Data Classification and Handling Policy for all ikaSystems employees, contractors, consultants, and business associates. ("Data Policy").

24. ikaSystems' Data Policy sets forth a four-tier classification scheme for all files: Public, Sensitive, Private, and Confidential. "Confidential" information is the highest level of classification reserved for the most sensitive ikaSystems information, and as such requires the strictest protection controls. This includes, but is not limited to, restricting access to only those on a "need to know" basis, limits on technical access, and all data must be encrypted both during transmission and at rest. Pursuant to the terms of this Data Policy, ikaSystems employees are required to clearly mark each file with one of the four classifications.

25. In order to enforce the Data Policy, ikaSystems uses Data Loss Prevention ("DLP") software that monitors all data activity within the company. The DLP software runs 24/7 on all ikaSystems computers, including both laptops and desktops. The DLP software monitors activity even when a corporate issued computer is not connected to the corporate network. All laptops are also enabled with disk encryption which requires an additional password

to unlock the computer before windows login. This mitigates unauthorized access to all data stored on the laptops.

26. Additionally, when a computer is connected to the corporate network, ikaSystems' firewall blocks access to unsecure sites, such as Google Drive, Dropbox, and other personal file sharing websites to prevent movement of protected data off the server to a non-protected location. This restriction prevents improper dissemination of confidential and proprietary information, PHI, and any other information not properly distributable under ikaSystems' Data Policy.

27. ikaSystems ensures all employees have knowledge of the Data Policy as well as all other corporate security protocols by mandating annual compliance training for all employees. ikaSystems may terminate employees who fail to complete this training. As an additional means of enforcing the Data Policy, each time an employee logs into the corporate network, the system generates an "acceptable use" prompt that requires the user to acknowledge ikaSystems' protocols for confidential information.

Kalidindi Gives Notice of His Resignation Then Immediately Begins Stealing ikaSystems' Trade Secrets

28. On or about July 29, 2018, Kalidindi gave ikaSystems notice he was leaving the company and his last day of employment would be August 17, 2018. (Resignation E-mail, attached as **Exhibit 2**.)

29. Soon after giving notice, and before his last day of employment, Kalidindi began secretly copying and transferring confidential files from the ikaSystems server.

30. The server activity on Kalidindi's laptop shows a sudden increase in internal file movements beginning on August 7, 2018. Specifically, Kalidindi moved files such as the "Visiant Data Modeling Standards" and "IT Efficiency Survey" to a "Planning" folder stored

locally on his laptop (the "Planning Folder"). In total, Kalidindi copied approximately 3,500 files to the Planning Folder. Many of these files included ikaSystems' highest level of data protection and confidential documents.

31. On August 14, 2018, Kalidindi transferred these files in bulk from his laptop to at least one personal Google Drive account, including the files identified above and hundreds of other files designated with ikaSystems' highest level of data protection and confidential files relating to ikaSystems' Enhanced Platform.

32. Kalidindi transferred this data when he was disconnected from the corporate network, which allowed him to access a restricted file-sharing website (Google Drive). ikaSystems' logs show many of these transfers occurring after 9:00 p.m. Because he transferred the information from a local drive when he was outside of the ikaSystems corporate network, ikaSystems did not immediately receive an alert that confidential or sensitive data was being transferred from a company computer to a third-party network.

33. Kalidindi transferred approximately 3,491 individual files totaling nearly 2 gigabytes of data. Approximately 1,930 of these documents contained protected material and 454 documents were marked "Confidential." Many of the documents contained valuable confidential and proprietary data, snippets of source code, database schemas, and information relating to the architectural design of the Enhanced Platform. These architecture documents constitute the key elements of ikaSystems' Enhanced Platform and they are some of the most valuable technical documents of the company.

34. In addition to the general confidential information, ikaSystems has been able to ascertain that Kalidindi transferred a file entitled "Future State Architecture Extension Final" ("Enhanced Platform Architecture") to his personal Google Account. This file provides the

blueprint to ikaSystems' Enhanced Platform project. It contains the architecture design of the software application and provides specific information on data flows and structures for how users interact. The document is several hundred pages long and contains valuable confidential and proprietary information.

35. Further, Kalidindi transferred documents to his Google Drive account that contained highly proprietary source code, database schema, financial data and other architecture documents for the Enhanced Platform, including a file entitled "ikaBilling – Domain Driven Design".

36. Kalidindi also transferred a file labeled "Production.docx" containing infrastructure diagrams, server names, configurations, security information, and other highly sensitive information. Additional transferred files relate to diagnostic codes for applications, financial information, and coding capabilities.

37. When Kalidindi began transferring these files to his personal Google Drive, he received DLP Alerts requesting the reason for the file transfers. Kalidindi responded to these alerts by entering into the ikaSystems system the following justification: "I did not know transferring this data was restricted". However, Kalidindi proceeded to transfer these files anyway, despite clear knowledge he was violating ikaSystems' Data Policy.

ikaSystems Receives Alerts for Kalidindi's Misappropriation and Kalidindi Lies and Destroys Evidence

38. On the morning of August 15, 2018, Mr. Kalidindi connected his ikaSystems issued laptop to the ikaSystems corporate network. At that point, ikaSystems immediately received DLP alerts advising it of Kalidindi's prohibited file transfers the previous evening.

39. As a result of the alerts, ikaSystems asked Kalidindi to bring his corporate laptop to ikaSystems' office for inspection. When Kalidindi initially refused this request, ikaSystems dispatched members of its corporate investigation team to Kalidindi's home to physically retrieve the laptop. While these ikaSystems employees were en route to Kalidindi's home, Kalidindi informed ikaSystems he would turn over the laptop.

40. That afternoon, Kalidindi returned his corporate laptop to ikaSystems. ikaSystems employees then interviewed Kalidindi about his file transfers. When confronted with information ikaSystems had uncovered from its DLP systems, Kalidindi acknowledged transferring ikaSystems data, but provided conflicting and varying statements regarding the type of data he transferred and the rational for the data transfers.

41. Kalidindi initially denied transferring any proprietary information from the network into his account, and claimed he only uploaded personal information he would need to access after he left ikaSystems. Kalidindi then admitted he moved architecture work and tools he developed during his employment at ikaSystems to his personal Google Drive.

42. Additionally, Kalidindi asserted he transferred some documents so he could later provide them to the ikaSystems employee who would replace him as lead architect on the Enhanced Platform project. This explanation, however, was implausible because, as detailed above, ikaSystems employees cannot access the Google Drive website from the ikaSystems

network. Further, Kalidindi's replacement had access to the confidential and proprietary information via the ikaSystems network.

43. During the interview, Kalidindi agreed to allow an ikaSystems employee to review the files on Kalidindi's Google Drive account. However, after opening the Google Drive account, Kalidindi claimed he had deleted almost all of the files prior to the interview. Kalidindi stated he realized he should not have uploaded the files and therefore purportedly deleted them from his personal Google Drive. Kalidindi was asked, and he repeatedly denied, having a second Google Drive account.

44. On information and belief, the reason Kalidindi originally refused to immediately provide his corporate laptop was to allow him sufficient time to delete the evidence of misappropriation from the Google accounts.

45. On August 17, 2018 – Kalidindi's last day of employment at ikaSystems – he participated in a follow-up interview, *i.e.* an "exit" interview. Kalidindi claimed it was a common practice for departing employees to take work tools that will assist them in a new job. Further, he falsely claimed he only uploaded "templates" he created which would be time-consuming to replicate at his new employer.

46. During this second interview, Kalidindi again permitted an ikaSystems employee to access his Google Drive account. While inspecting the Google Drive, the ikaSystems employee noticed that the account's history had been cleared approximately 15 minutes before the interview. This history would have provided an audit trail detailing when the misappropriated information was uploaded to the Google Drive account and if the information had been transferred and/or deleted. Again, Kalidindi represented that this was the only Google Drive account involved in the file transfers.

47. However, after the interview, ikaSystems' investigation revealed that Kalidindi accessed a second Google Drive account from his ikaSystems computer. Kalidindi intentionally hid the existence of this account from ikaSystems.

ikaSystems has been, and will be, severely harmed by Kalidindi's Misappropriation of ikaSystems' Confidential Trade Secret Information

48. Because of Kalidindi's misrepresentations to ikaSystems regarding his transfer of ikaSystems' confidential trade secret information, it is unclear what remains on Kalidindi's Google Drive account or whether Kalidindi has again moved these files to another location.

49. The storage of ikaSystems' classified files on a public file sharing server such as Google Drive creates an immense information security risk to ikaSystems. These files could become public and indexed by Google's search engine, and thus available to anyone on the internet.

50. Additionally, the ikaSystems trade secrets discussed above have value from not being known, except to those limited ikaSystems employees who need to know. Once the trade secrets become known publically, or known to an ikaSystems competitor, they lose all value.

COUNT I
VIOLATION OF THE DEFEND TRADE SECRETS ACT OF 2016
(18 U.S.C. § 1836)

51. ikaSystems incorporates herein all other allegations of this Complaint.

52. ikaSystems owns and possesses architectural designs and source code for proprietary software platforms constituting confidential and trade secret information, including, (i) the Enhanced Platform's architectural software design, specific data flows, and user interaction structures contained in the "Future State Architecture Extension Final" document; (ii) the Enhanced Platform's proprietary source code and database schema; and (iii) the

infrastructure diagrams, configurations, and security information contained in the "Production" document.

53. ikaSystems took reasonable steps to protect and maintain the secrecy of its trade secrets, including requiring its employees to agree to keep such information confidential in their employment agreements, instituting a strict information protection policy that required classification of all confidential information, enforcing the policy by constantly monitoring all employee activity on corporate devices, establishing an alert system to flag any potential violations of the policy, and requiring all employees to complete annual training on ikaSystems' information protection policy and procedures.

54. ikaSystems' misappropriated confidential and trade secret information relates to products and services used in interstate commerce. ikaSystems' trade secrets derive independent economic value from not being generally known to, and not being readily ascertainable through proper means by, another person who could obtain economic value from the disclosure or use of the information.

55. Kalidindi, through improper means, including but not limited to breaching confidentiality agreements and ikaSystems' data protection policy, improperly acquired, used, and/or disclosed ikaSystems' confidential trade secret information in direct violation of Kalidindi's obligations under his confidentiality agreement and ikaSystems' policies.

56. As a direct and proximate result of Kalidindi's conduct, IkaSystems has suffered and will continue to suffer, severe harm, irreparable injury, and significant damages.

57. Kalidindi's misappropriation of ikaSystems' trade secrets was willful and malicious, and ikaSystems is entitled to an award of exemplary damages and attorneys' fees.

COUNT II
MASSACHUSETTS TRADE SECRET MISAPPROPRIATION
(M.G.L. C. 93, § 42)

58. ikaSystems incorporates herein all other allegations of this Complaint.

59. ikaSystems owns and possesses architectural designs and source code for proprietary software platforms constituting confidential trade secret information, including, (i) the Enhanced Platform's architectural software design, specific data flows, and user interaction structures contained in the "Future State Architecture Extension Final" document; (ii) the Enhanced Platform's proprietary source code and database schema; and (iii) the infrastructure diagrams, configurations, and security information contained in the "Production" document.

60. ikaSystems took reasonable steps to protect and maintain the secrecy of its trade secrets, including requiring its employees to agree to keep such information confidential in their employment agreements, instituting a strict information protection policy that required classification of all confidential information, enforcing the policy by constantly monitoring all employee activity on corporate devices, establishing an alert system to flag any potential violations of the policy, and requiring all employees to complete annual training on ikaSystems' information protection policy and procedures.

61. ikaSystems' trade secrets derive independent economic value from not being generally known to, and not being readily ascertainable through proper means by, another person who could obtain economic value from the disclosure or use of the information.

62. Kalidindi, through improper means, including but not limited to breaching confidentiality agreements and ikaSystems' data protection policy, improperly acquired, used, and/or disclosed ikaSystems' confidential trade secret information in direct violation of Kalidindi's obligations under his confidentiality agreement and ikaSystems' policies.

63. As a direct and proximate result of Kalidindi's conduct, ikaSystems has suffered and will continue to suffer severe harm, irreparable injury, and significant damages.

COUNT III
BREACH OF CONTRACT

64. ikaSystems incorporates herein all other allegations of this Complaint.

65. The Non-Competition, Non-Solicitation, and Confidentiality Agreement ("Agreement") is valid and enforceable.

66. Kalidindi acknowledged in the Agreement he owed a duty of loyalty to ikaSystems and he would not take any action that could adversely affect the company.

67. Kalidindi breached his duty of loyalty to ikaSystems by improperly acquiring ikaSystems' valuable and proprietary confidential information.

68. Kalidindi acknowledged in the Agreement he would have access to confidential and proprietary information and agreed not to use or disclose any of this information for any purpose other than the performance of his essential job duties at ikaSystems.

69. Kalidindi breached the Agreement by improperly acquiring, using, and/or disclosing confidential and proprietary information, for his own personal use and other purposes outside of the performance of his essential job duties at ikaSystems.

70. In the Agreement, Kalidindi agreed that all intellectual property developed in the course of his employment, including software code and similar developments, shall remain the property of ikaSystems.

71. Kalidindi breached the Agreement by improperly acquiring intellectual property developed in the course of his employment.

72. In the Agreement, Kalidindi agreed that upon termination, he would return to ikaSystems all confidential information, including documents, notes, models, and any other data and records of any kind.

73. Kalidindi breached the Agreement by transferring ikaSystems' confidential information to his personal Google Drive account.

74. Kalidindi also breached the Agreement by failing to return all confidential information to ikaSystems.

75. ikaSystems performed all obligations to Kalidindi under the Agreement.

76. Kalidindi failed to perform his obligations to ikaSystems under the Agreement.

77. As a result of Kalidindi's breach of his contractual obligations to ikaSystems under the Agreement, ikaSystems has been and will continue to be irreparably damaged.

COUNT IV
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

78. ikaSystems incorporates herein all other allegations of this Complaint.

79. At all material times, ikaSystems properly and fully performed its obligations under the Agreement.

80. The Agreement was supported by sufficient consideration and was entered into knowingly and voluntarily by Kalidindi.

81. Kalidindi owed a duty of good faith and fair dealing to ikaSystems.

82. As set forth above, Kalidindi's actions, including but not limited to, improperly acquiring, using, and/or disclosing ikaSystems' confidential and proprietary information, and failing to return this information to ikaSystems upon Kalidindi's termination, violated his duty of good faith and fair dealing by injuring ikaSystems' right to receive the benefits of the Agreement and breached the implied covenant of good faith and fair dealing.

83. As a direct and proximate result of Kalidindi's conduct, ikaSystems has been and will continue to be irreparably harmed.

COUNT V
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
(18 U.S.C. § 1030, *ET SEQ.*)

84. ikaSystems incorporates herein all other allegations of this Complaint.

85. ikaSystems' computer system comprises a protected computer that is used in and affects interstate commerce.

86. By the conduct described above, Kalidindi knowingly and with intent to defraud, accessed ikaSystems' protected computer system, without authorization and/or in excess of his authorized access, for his own benefit, and thereby obtained information from a protected computer.

87. Kalidindi knowingly caused the transmission of information that intentionally caused damage, without authorization, to ikaSystems.

88. Kalidindi's conduct caused loss or damage to ikaSystems in excess of $5,000.

89. As a direct and proximate result of Kalidindi's conduct, ikaSystems has suffered and will continue to suffer substantial direct and consequential damages and irreparable harm.

COUNT VI
CONVERSION

90. ikaSystems incorporates herein all other allegations of this Complaint.

91. ikaSystems had possession, or a right of immediate possession, of the confidential and proprietary information that was available to Kalidindi through his work for ikaSystems.

92. Kalidindi converted ikaSystems property and confidential information to his own use by exercising dominion over the property in violation of Kalidindi's obligations and duties to ikaSystems.

93. As a direct and proximate cause of Kalidindi's wrongful conduct, ikaSystems has suffered and will continue to suffer substantial direct and consequential damages and irreparable harm.

PRAYER FOR RELIEF

WHEREFORE*,* ikaSystems respectfully requests that this Court grant ikaSystems the following relief:

A. Judgment in ikaSystems' favor and against Kalidindi on all causes of action alleged herein;

B. A Temporary Restraining Order:

(i) Prohibiting Kalidindi's conduct described herein;

(ii) Prohibiting Kalidindi and all persons acting in concert or participation with him, including any officer, agent, employee, or attorney, be enjoined from using, copying, viewing or disclosing, for any purpose, any confidential, proprietary, or trade secret information belonging to ikaSystems;

(iii) Requiring Kalidindi to immediately identify any individual or entity to whom ikaSystems' confidential, proprietary, or trade secret information has been disclosed or otherwise transferred;

(iv) Requiring Kalidindi to identify to ikaSystems' counsel within 7 days any and all electronic files, documents and other information taken from ikaSystems and the locations of all such information, including any Google drives or other third-party storage devices or drives;

(v) Requiring Kalidindi to provide to ikaSystems' counsel within 7 days a detailed accounting of how and when Kalidindi, or anyone acting in concert or participation with him, has used, accessed, copied or viewed any portion of any electronic files, documents or information taken from ikaSystems;

(vi) Requiring Kalidindi to maintain and preserve all materials of any kind taken by Kalidindi from ikaSystems, all evidence of the circumstances of such taking, including all incidents of downloading and/or copying, all material concerning ikaSystems maintained in any electronic form, including evidence that may be stored on Kalidindi's Google accounts or other shared storage locations, all computers, laptop computers, smart phones, tablets, hard drives, zip drives, CDs or other devices in his possession, custody or control on which electronic files may be stored, copied or accessed;

(vii) Granting ikaSystems leave to serve limited nonparty subpoenas to understand the scope of Kalidindi's misappropriation and prevent the destruction of evidence, pursuant to FRCP 26(d)(1);

(viii) Requiring Kalidindi to permit within 7 days a third-party forensic investigator chosen by ikaSystems to inspect Kalidindi's Google accounts or other shared storage locations, and all computers, laptop computers, smart phones, tablets, hard drives, zip drives, CDs or other devices in Kalidindi's possession, custody or control on which electronic files may be stored, copied or accessed;

(ix) Requiring Kalidindi produce and respond to the early emergency;

(x) Requiring Kalidindi show cause why a preliminary injunction should not issue;

C. A preliminary and permanent injunction prohibiting Kalidindi's conduct described herein, prohibiting and further use, accessing, or dissemination of ikaSystems' confidential information, and requiring the return and/or destruction of any and all copies of ikaSystems' confidential information in existence as a result of or stemming from the misconduct complained of herein;

D. Damages in an amount to be proven;

E. Double the amount of damages proven;

F. Punitive damages;

G. Restitution;

H. The costs of suit incurred herein, including attorneys' fees and costs;

I. Prejudgment interest;

J. Seizure of all media, storage devices or other property on which ikaSystems' confidential information is stored as a result of Kalidindi's misconduct; and

K. Such other and further relief as the Court may deem to be just and proper.

Respectfully submitted:

By: /s/ Eric Osterberg
Eric Osterberg (BBO# 624944)
OSTERBERG LLC
50 Milk Street, 16th Floor,
Boston, MA 02109
617-294-6542
eosterberg@osterbergllc.com

DICKINSON WRIGHT PLLC

John S. Artz (Pro Hac Pending)
Peter E. Doyle (Pro Hac Pending)
2600 W. Big Beaver Rd., Ste. 300
Troy, Michigan 48084
(248) 433-7200
jsartz@dickinsonwright.com
pdoyle@dickinsonwright.com

Steven A. Caloiaro (Pro Hac Pending)
100 W. Liberty Street
Reno, NV 89501
(775) 343-7500
Scaloiaro@dickinsonwright.com

September 10, 2018